ABSTRACT

This invention describes and specifies a cryptographic method/system employing one-way invertible transforms. In one embodiment, many different encryption keys can correspond to one single decryption key that decrypts different versions of ciphertext created by the many different encryption keys uniquely to the original plaintext; and in another embodiment one single encryption key can correspond to many different decryption keys that give different decrypted results. The encryption key is so constructed that it allows a high level of parallel computation.